RECEIVED
CENTRAL FAX CENTER

DEC 2 8 2005



Appl. No. 09/275,722

Attorney Docket: 042390.P6526

In The United States Patent and Trademark Office
Before The Board of Patent Appeals and Interferences

| | | | |
|---|---|---|---|
| In re Patent Application of: | Lee, David A. | Examiner: | Gyorfi, Thomas A. |
| | | Art Unit: | 2135 |
| Application No.: | 09/275,722 | | |
| Filed: | March 24, 1999 | | |
| For: | A METHOD AND APPARATUS FOR THE GENERATION OF CRYPTOGRAPHIC KEYS | | |

**APPEAL BRIEF**
**IN SUPPORT OF APPELLANTS' APPEAL**
**TO THE BOARD OF PATENT APPEALS AND INTERFERENCES**

Honorable Director of the United States Patent and Trademark Office
Washington, DC 20231

Sir/Madam:

Applicant (hereafter "Appellant") hereby submits this Brief in support of their Appeal from a final decision by the Examiner in the above-captioned case. Appellant respectfully requests consideration of this Appeal by the Board of Patent Appeals and Interferences for allowance of the claims in the above-captioned patent application.

An oral hearing is not desired.

# TABLE OF CONTENTS

## 1. REAL PARTY IN INTEREST

The invention is assigned to Intel Corporation of 2200 Mission College Boulevard, Santa Clara, California 95052.

## 2. RELATED APPEALS AND INTERFERENCES

To the best of Appellants' knowledge, there are no appeals or interferences related to the present appeal that will directly affect, be directly affected by, or have a bearing on the Board's decision.

## 3. STATUS OF THE CLAIMS

Claims 1-27 are now pending in the above referenced patent application. Claims 1-27 were rejected for the third time in the Office Action mailed on August 10, 2005 and are the subject of this appeal.

## 4. STATUS OF THE AMENDMENTS

No amendments have been filed subject to the Final Rejection.

A copy of all claims on appeal is attached hereto as Appendix A.

## 5. SUMMARY OF THE CLAIMED SUBJECT MATTER

In today's society, it is becoming more and more desirable to transmit digital information from one location to another in a manner that is clear and unambiguous to a legitimate receiver, but incomprehensible to any illegitimate recipients. Accordingly, such information is typically encrypted using one of two commonly used cryptographic techniques: public key cryptography and symmetric key cryptography. (Appellant's Specification, page 1.)

In general, public key cryptography involves the use of a public key and a private key (collectively referred to as a "key pair") which are two separate, but related keys. Normally, the public key is publicly available and widely used for encrypting a message directed to the owner of the key pair. The private key is maintained in confidence and usually is used for decryption of incoming encrypted message. As a result, public key cryptography tends to be more secure than symmetric key cryptography, but it is more cumbersome and computationally intensive. The intense computations tend to prevent consumer electronic devices and other lower performance devices from using public key cryptography. (Appellant's Specification, page 2.)

With respect to cryptography related terminology, the term "secure" indicates a state where it is not reasonably feasible for an unauthorized individual to access information in an non-encrypted format. A "key" is generally defined as an encoding and/or decoding parameter usually structured as a sequence of binary data. A "digital signature" includes digital information signed with a private key of its signatory to ensure that the digital information has not been illicitly modified after being digitally signed. This digital information may be provided in its entirety or as a digest produced by a one-way hash function. The "one-way hash function" includes a function, mathematical or otherwise, that converts information from a variable-length to a fixed-length (referred to as a "digest"). The term "one-way" indicates that there does not

readily exist an inverse function to recover any discernible portion of the original information from the fixed-length digest. Examples of a hash function include MD2 or MD5 provided by RSA Data Security of Redwood City, California, or Secure Hash Algorithm (SHA-1) as specified by the National Institute of Standards and Technology located in Washington, D.C.

In addition, a "digital certificate" includes digital information used to authenticate a sender of information. For example, a digital certificate may include information concerning a person, entity or device being certified that is encrypted with the private key of a certification authority. Examples of a "certification authority" include an original equipment manufacturer (OEM), a software vendor, a trade association, a governmental entity, a bank or any other trusted business or person.

Referring now to Figure 1, an illustrative block diagram of an embodiment of a network 100 employing at least two digital platforms is shown. Network 100 includes a first digital platform 120 and a second digital platform 130 capable of establishing communications with certification authority 110 via channels 140 and 150, respectively. Platforms 120 and 130 can register with certification authority 110 in order to receive secret device keys therefrom. Each platform 120 or 130 can be classified as either (i) an information provider, or (ii) an information receiver, or (iii) a transceiver capable of operating as either an information provider or an information receiver. Of course, other classification schemes may be utilized so long as communicative platforms have compatible classifications. Also, first and second digital platforms 120 and 130 communicate with each other via channel 160.

As shown in Figure 2, an embodiment of certification authority 110 is shown. Certification authority 110 comprises a digital platform that includes a processing unit 200 and memory 210. In particular, processing unit 200 is any hardware having code processing

capabilities such as, for example, a central processing unit, a microcontroller, a coprocessor, a state machine and the like. Processing unit 200 accesses information from memory 210. In one embodiment, memory 210 is volatile memory with data backed-up in non-volatile storage. Of course, it is contemplated that memory 210 may be implemented to operate as non-volatile memory to ensure that its contents are retained during a power-down condition. Thus, memory 210 may include, for example, (i) read only memory (ROM), (ii) any type of programmable read only memory (PROM) such as erasable PROM (EPROM) or electrically erasable PROM (EEPROM), (iii) flash memory, or even (iv) battery-backed volatile memory.

Memory 210 retains the certification authority's public key (PUKCA) 220, its private key (PRKCA) 230, and a multi-dimensional matrix 240 of matrix keys (K) arranged in grids (e.g., rows, columns, along z-axis, etc.) held in secret to be known only by certification authority 110 of Figure 1. PUKCA 220 and PRKCA 230 are provided to support matrix key authentication schemes, not the formation of shared secret key "SECKEY". Currently, each key is 64-bits, although any bit size may be used (e.g., 32, 128, 160, 256, 512, 1024...). For increased protection, PRKCA 230 and key matrix 240 may be obfuscated by tamper-resistant software. The dimensions of key matrix 240 and length of the matrix keys correspond to the desired strength of security for network 100 of Figure 1.

In the event that key matrix 240 is a two-dimensional nxm matrix, for example, one matrix dimension (e.g., "n" rows) may be assigned to a first platform classification while the other matrix dimension (e.g., "m" columns) is assigned to a second platform classification. The "platform classifications" need only be something that can differentiate participants of the authentication. Thus, the classification may be (1) information provider/information receiver; (2) multiple types of information providers; and (3) multiple types of information receivers and

the like. Thus, if the first platform classification is an information provider, it would receive "m" secret device key sets created by performing arithmetic operations on the matrix keys situated in selected "p" rows (p<n) for each column. For this embodiment, the arithmetic operation involves modular addition, although exclusive-or (XOR) operations, non-modular addition or other operations may be used. Information receivers (second class), however, would receive "n" secret device key sets created by performing arithmetic operations on the matrix keys situated in selected "q" columns (q<m) for each row. For maximum security, "p" is equal to $\frac{n}{2}$ and "q" is equal to $\frac{m}{2}$; however, p or q may be any selected number of rows or columns less than n or m, respectively (see Figure 6).

Referring now to Figure 3, an illustrative block diagram of a first embodiment of key matrix 240 is shown. Key matrix 240 is a two-dimensional, nxm matrix with a first dimension (e.g., rows) 300 dedicated to a first platform classification (e.g., an "information provider" class) and a second dimension (e.g., columns) 310 dedicated to a second platform classification (e.g., an "information receiver" class). For clarity sake, key matrix 240 is represented as a 6x6 matrix; however, key matrix 240 normally comprises a larger-sized matrix, even a 40x40 matrix or larger. It is contemplated that the dedication of matrix dimensions for each class could be different. For example, columns and rows could be dedicated to the "information provider" and "information receiver" classes, respectively.

For each digital platform, the certification authority generates a combination of rows or columns associated with key matrix 240. Preferably, the combination is unique, but uniqueness is not required. For example, in this embodiment, if the first digital platform is classified as an information provider, the certification authority generates a combination of rows, which is

represented as a first key selection vector (KSV1) 320 for the first digital platform. Herein, KSV1 320 is equal to <2, 3, 5>. Based on KSV1 320, the certification authority generates a set of secret device keys (1_SDKEY1 - 1_SDKEY6) 330-335 and provides both KSV1 320 and the first set of secret device keys 330-335 to the first digital platform. As shown in Figure 4, secret device keys 330-335 are generated through modular addition (e.g., modulo $2^{64}$) of matrix keys in the selected rows of key matrix 240 for each column.

Referring back to Figure 3, if the second digital platform is classified as an information receiver, the certification authority generates a combination of columns associated with key matrix 240, which is represented as a second key selection vector (KSV2) 340. Herein, KSV2 340 is equal to <1, 3, 4>. Based on KSV2 340, certification authority generates a set of secret device keys (2_SDKEY1 - 2_SDKEY6) 350-355 and provides both KSV2 340 and the set of secret device keys 350-355 to the second digital platform. As shown in Figure 5, for each row, the second set of secret device keys 350-355 are produced through modular addition of the matrix keys of key matrix 240 pertaining to those columns selected by KSV2 340.

To secure channel 160 of Figure 1, the first and second digital platforms exchange KSV1 320 and KSV2 340. Hence, based on KSV2 340, the first digital platform creates a shared secret key (SECKEY) equivalent to the modular addition of 1_SDKEY1, 1_SDKEY3 and 1_SDKEY4. Concurrently, based on KSV1 320, the second digital platform also produces SECKEY through modular addition of 2_SDKEY2, 2_SDKEY3 and 2_SDKEY5. As shown in equation (1), SECKEY is determined to be the following:

$$(1) \quad \text{SECKEY (at DP1)} = (K21+K31+K51)+(K23+K33+K53)+(K24+K34+K54)$$
$$= (K21+K23+K24)+(K31+K33+K34)+(K51+K53+K54)$$

Referring now to Figure 6, an illustrative block diagram of a second embodiment of key matrix 240 is shown. Key matrix 240 is a two-dimensional, n×m matrix with a first dimension (e.g., rows) 400 dedicated to the "information provider" class and a second dimension (e.g., columns) 410 dedicated to the "information receiver" class. For clarity sake, key matrix 240 is represented as a rectangular (4×5) matrix in lieu of a square (6×6) matrix as shown in Figure 3. (Appellant's Specification, pages 7-12.)

Referring now to Figure 9, an illustrative block diagram of a third embodiment of key matrix 240 is shown. Key matrix 240 is a two-dimensional, n×m matrix with a first dimension (e.g., rows) 500 dedicated to the "information provider" class and a second dimension (e.g., columns) 510 dedicated to the "information receiver" class. For clarity sake, key matrix 240 is symmetric and represented as a 4×4 matrix. (Appellant's Specification, page 13.)

## 6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The above referenced patent application has been reviewed in light of the Office Action, dated August 10, 2005, in which:

- claims 1-18 are rejected under 35 U.S.C. § 101 as having no utility;
- claim 19 is objected to because of a lack of antecedent basis;
- claims 1, 3-11, and 13-27 are rejected under 35 U.S.C. § 102(e) on Lotspiech *et al.* (hereinafter 'Lotspiech;' U.S. Patent No. 6,118,873);
- and claims 2 and 12 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Lotspiech in combination with Luther (U.S. Patent No. 5,533,127).

# 7. ARGUMENT

## *7.1. Claim Objections*

### 7.1.1. Claim 19

The PTO has objected to claim 19 because "there appears to be no antecedent basis for the limitation 'machine readable medium'". This objection is respectfully traversed.

M.P.E.P. § 2173.05(e) addresses a lack of antecedent basis.

> **2173.05(e) Lack of Antecedent Basis**
>
> A claim is indefinite when it contains words or phrases whose meaning is unclear. The lack of clarity could arise where a claim refers to "said lever" or "the lever," where the claim contains no earlier recitation or limitation of a lever and where it would be unclear as to what element the limitation was making reference. Similarly, if two different levers are recited earlier in the claim, the recitation of "said lever" in the same or subsequent claim would be unclear where it is uncertain which of the two levers was intended. A claim which refers to "said aluminum lever," but recites only "a lever" earlier in the claim, is indefinite because it is uncertain as to the lever to which reference is made. Obviously, however, the failure to provide explicit antecedent basis for terms does not always render a claim indefinite. If the scope of a claim would be reasonably ascertainable by those skilled in the art, then the claim is not indefinite. *Ex parte* Porter, 25 USPQ2d 1144, 1145 (Bd. Pat. App. & Inter. 1992) ("controlled stream of fluid" provided reasonable antecedent basis for "the controlled fluid"). Inherent components of elements recited have antecedent basis in the recitation of the components themselves. For example, the limitation "the outer surface of said sphere" would not require an antecedent recitation that the sphere has an outer surface.
>
> **A CLAIM TERM WHICH HAS NO ANTECEDENT BASIS IN THE DISCLOSURE IS NOT NECESSARILY INDEFINITE**
>
> The mere fact that a term or phrase used in the claim has no antecedent basis in the specification disclosure does not mean, necessarily, that the term or phrase is indefinite. There is no requirement that the words in the claim must match those used in the specification disclosure. Applicants are given a great deal of latitude in how they choose to define their invention so long as the terms and phrases used define the invention with a reasonable degree of clarity and precision.

Appellant begins with claim 19. Claim 19 recites:

19. A machine readable medium having embodied thereon a computer program for processing by a first digital platform including memory containing the computer program comprising:

an authentication function to recover an incoming key selection vector and to compute a shared secret key based on a set of secret device keys stored in the first digital platform and the contents of the incoming key selection vector;

a transfer function to output at least a key selection vector assigned to the first digital platform;

a hash function to perform a hash operation on at least the shared secret key to produce a resultant hash value; and

a comparison function to compare the resultant hash value with an incoming check hash value received subsequent to the transmission of the key selection vector.

Appellant respectfully asserts that antecedent basis for "machine readable medium" may be found in the first 3 words of line 1, "A machine readable medium".

Furthermore, Appellant asserts that the plain, dictionary meaning of the phrase renders the phrase sufficiently clear to overcome this objection. See M.P.E.P. § 2111. It is respectfully asserted the phrase obviously means "a medium which is able to be read by a machine". The American Heritage Dictionary of the English Language, 3rd ed., 1996 by Houghton Mifflin Company defines a "medium" as "an intervening substance through which something else is transmitted or carried on."

Appellant respectfully asserts that, when given the broadest reasonable interpretation and plain dictionary meaning, the objected phrase does not lack antecedent basis. It is, therefore, respectfully requested that the objection of this claim be withdrawn.

## *7.2. 35 U.S.C. § 101*

### 7.2.1. Claims 1-18

The PTO has rejected claims 1-18 under 35 U.S.C. § 101. This rejection by the PTO of these claims is respectfully traversed.

As a procedural matter and to aid clarification, it is also respectfully noted that this rejection was raised and successfully overcome in the May 27, 2003 Office Action and subsequent Reply. Over two years later this rejection reappeared in the August 10, 2005 Office Action.

35 U.S.C. § 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefore, subject to the conditions and requirements of this title.

M.P.E.P. § 2107.02 sets forth the standard for a § 101 rejection based upon utility:

> **2107.02 Procedural Considerations Related to Rejections for Lack of Utility**
>
> **An Asserted Utility Creates a Presumption of Utility**
>
> In most cases, an applicant's assertion of utility creates a presumption of utility that will be sufficient to satisfy the utility requirement of 35 U.S.C. 101. See, e.g., In re Jolles, 628 F.2d 1322, 206 USPQ 885 (CCPA 1980); In re Irons, 340 F.2d 974, 144 USPQ 351 (CCPA 1965); In re Langer, 503 F.2d 1380, 183 USPQ 288 (CCPA 1974); In re Sichert, 566 F.2d 1154, 1159, 196 USPQ 209, 212-13 (CCPA 1977). As the Court of Customs and Patent Appeals stated in In re Langer:
>
> As a matter of Patent Office practice, a specification which contains a disclosure of utility which corresponds in scope to the subject matter sought to be patented must be taken as sufficient to satisfy the utility requirement of § 101 for the entire claimed subject matter unless there is a reason for one skilled in the art to question the objective truth of the statement of utility or its scope.

Appellant respectfully asserts that the claims 1 & 11 result in a "shared secret key." One of the uses of the claimed invention is explicitly recited in the specification on page 3, lines 1-5. "[I]t would be desirable to develop a cryptographic technique that provides the security advantages of public key cryptography without the disadvantages of being cumbersome and computationally intensive." It is noted that the stated use is merely one of the possible uses for the "shared secret key," and the invention is not limited to the cited use. Appellant respectfully reiterates the directive of M.P.E.P. § 2107.02 "As a matter of Patent Office practice, a specification which contains a disclosure of utility which corresponds in scope to the subject matter sought to be patented **must be taken** as sufficient to satisfy the utility requirement of § 101 for the entire claimed subject matter." (emphasis added)

It is respectfully asserted that the PTO has failed to support a proper § 101 rejection for a variety of reasons. Likewise, claims 2-10 and 12-18 are patentable for similar reasons. It is, therefore, respectfully requested that the rejection of these claims also be withdrawn.

## *7.3. 35 U.S.C. § 102(b)*

### 7.3.1. Lotspiech: Claims 1, 3-11, and 13-27

The PTO has rejected claims 1, 3-11, and 13-27 under 35 U.S.C. § 102(b) as being anticipated by Lotspiech. This rejection by the PTO of these claims is respectfully traversed.

It is well-established that in order to establish a *prima facie* case of anticipation under § 102 of the patent statute, the PTO must provide a single prior art document that alone has every element and every limitation of the claim being rejected. Therefore, if even a single element or limitation is not met by the asserted document, then the PTO has not succeeded in establishing a prima facie case.

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *Verdegaal Brothers v. Union Oil Co. of California*, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). The identical invention must be shown in as complete detail as is contained in the claim. *Richardson v. Suzuki Motor Co.*, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

Appellant begins with claim 1. Claim 1 recites:

1. A method comprising:
providing a key matrix having N rows and M columns of matrix keys, where N≥2 and M≥2;
dedicating the rows of the key matrix to a first classification;
for each column of the key matrix, performing arithmetic operations utilizing matrix keys of at least two selected rows of the key matrix to produce a secret device key which is part of a first set of secret device keys;
producing a shared secret key based on arithmetic operations on selected secret device keys of the first set of secret device keys.

It is respectfully asserted that, as just one example of how the text cited by the PTO fails to meet the language of the rejected claims, Lotspiech does not show, teach, use, or describe

utilizing matrix keys of **at least two selected rows** of the key matrix **to produce a secret device key**. The PTO states that Lotspiech shows this feature on Column 5, lines 55-68, but Appellant respectfully asserts that Lotspiech does not show this.

Lotspiech, in Column 5, lines 55-68, describes the creation of the matrix illustrated by Lotspiech Fig. 5. An important thing to notice from Fig. 5 is that the elements (*e.g.* $E(x_1, s_{1,1})$) consist of results derived **not from at least two rows** of what the PTO contends is Lotspiech's key matrix (Fig. 3), but **one element of the key matrix**, $s_{1,1}$, and a session number, $x_1$. See, Col. 5, line 60. It is respectfully asserted that if at least two rows were used the elements of Fig. 5 would consist of results derived from functions that require multiple key matrix elements as inputs, such as, for example, $E(x_1, s_{1,1}, s_{1,2})$. In contrast, Appellant's Fig. 5 illustrates taking multiple rows (three in the case of Fig 5) from the key matrix and using them to produce a secret device key, such as, for example, $2\_SDKEY1 = K_{11} + K_{13} + K_{14}$, which is part of a fist set of secret device keys. Therefore, it is respectfully asserted that Lotspiech fails to satisfy a *prima facie* case of anticipation as directed by 35 U.S.C. § 102.

Claims 3-11 and 13-27 either depend from claim 1, or include a substantially similar and patentably distinct limitation as claim 1. It is, therefore, respectfully requested that the rejection of these claims also be withdrawn.

## *7.4. 35 U.S.C. § 103(a)*

### 7.4.1. Lotspiech and Luther: Claims 2 and 12

The PTO has also rejected claims 2 and 12 under 35 U.S.C. § 103(a) based upon Lotspiech in combination with Luther. The rejection of these claims is respectfully traversed.

M.P.E.P. § 706.02(j) sets forth the standard for a § 103(a) rejection:

> To establish a prima facie case of obviousness, three basic criteria must be met.
>
> First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or combine reference teachings.
>
> Second, there must be a reasonable expectation of success.
>
> Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.
>
> The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991) (whitespace added).

Appellant begins with claim 2. Claim 2 recites:

> (Original) 2. The method of claim 1, wherein the arithmetic operations include modular addition.

Claim 2 ultimately depends upon claim 1. Claim 1 recites:

> 1. A method comprising:
>
> providing a key matrix having N rows and M columns of matrix keys, where N≥2 and M≥2;
>
> dedicating the rows of the key matrix to a first classification;
>
> for each column of the key matrix, performing arithmetic operations utilizing matrix keys of at least two selected rows of the key matrix to produce a secret device key which is part of a first set of secret device keys;
>
> producing a shared secret key based on arithmetic operations on selected secret device keys of the first set of secret device keys.

Appellant respectfully asserts that the combination set forth by the PTO fails to meet the requirement for a *prima facie* case for a § 103(a) rejection for at least the following reasons.

It is respectfully asserted that neither Lotspiech nor Luther, either alone or in combination, suggests or describes utilizing matrix keys of **at least two selected rows** of the key matrix **to produce a secret device key**. See discussion above. It is, therefore, respectfully requested that the rejection of this claim be withdrawn.

Claims 12 either depends from and include the limitations of claim 2, or includes a substantially similar and patentably distinct limitation as claim 2. Therefore, these claims patentably distinguish from the cited patents on the same basis as claim 2. It is, therefore, respectfully requested that the PTO withdraw the rejections of these claims.

## 8. CONCLUSION

In view of the foregoing, it is respectfully asserted that all claims pending in this application, as amended, are in condition for allowance. If the Examiner has any questions, they are invited to contact the undersigned at 503-264-7002. Reconsideration of this patent application and early allowance of all claims is respectfully requested.

Respectfully submitted,

Dated: Wed Dec 28, 2005

Justin B. Scout
Reg. No. 54,431

c/o Blakely, Sokoloff, Taylor & Zafman, LLP
12400 Wilshire Blvd., Seventh Floor
Los Angeles, CA 90025-1026
(503) 264-0967

# APPENDIX A: CLAIMS APPENDIX

(Previously Presented) 1. A method comprising:

providing a key matrix having N rows and M columns of matrix keys, where N≥2 and M≥2;

for each column of the key matrix, performing arithmetic operations utilizing matrix keys of at least two selected rows of the key matrix to produce a secret device key which is part of a first set of secret device keys;

producing a shared secret key based on arithmetic operations on selected secret device keys of the first set of secret device keys.

(Original) 2. The method of claim 1, wherein the arithmetic operations include modular addition.

(Original) 3. The method of claim 1, wherein prior to performing the arithmetic operations, the method comprises:

generating a key selection vector identifying the at least two selected rows of the key matrix from which to produce the first set of secret device keys.

(Original) 4. The method of claim 3, wherein the key selection vector is uniquely assigned to a first digital platform.

(Original) 5. The method of claim 4, wherein prior to producing the shared secret key, the method comprises:

receiving a key selection vector from a second digital platform in communication with the first digital platform; and

analyzing contents of the key selection vector from the second digital platform to determine the selected secret device keys of the first set of secret device keys.

(Original) 6. The method of claim 1, wherein prior to performing arithmetic operations on keys of at least two selected rows, the method further comprises:

dedicating the rows of the key matrix to a first classification; and

dedicating the columns of the key matrix to a second classification.

(Original) 7. The method of claim 6, wherein the first classification includes digital platforms designed to provide information to other digital platforms.

(Original) 8. The method of claim 7, wherein the second classification includes digital platforms designed to receive information from other digital platforms.

(Original) 9. The method of claim 1, wherein the producing of the shared secret key comprises:

analyzing contents of an incoming key selection vector; and

performing arithmetic operations of the selected secret device keys located in columns of the key matrix identified by the contents of the incoming key selection vector.

(Original) 10. The method of claim 9, wherein the producing of the shared secret key further comprises:

performing a hash operation on results of the arithmetic operations of the selected secret device keys located in the column of the key matrix identified by the contents of the incoming key selection vector.

(Previously Presented) 11. A method comprising:

providing a key matrix having N rows and M columns of matrix keys, where N≥2 and M≥2;

for each row of the key matrix, performing arithmetic operations utilizing matrix keys of at least two selected columns of the key matrix to produce a secret device key which is part of a first set of secret device keys;

producing a shared secret key based on arithmetic operations on selected secret device keys of the first set of secret device keys.

(Original) 12. The method of claim 11, wherein the arithmetic operations include modular addition.

(Previously Presented) 13. The method of claim 11, wherein prior to performing the arithmetic operations, the method comprises:

generating a key selection vector identifying the at least two selected columns of the key matrix from which to produce the first set of secret device keys.

(Original) 14. The method of claim 13, wherein the key selection vector is uniquely assigned to a first digital platform.

(Original) 15. The method of claim 14, wherein prior to producing the shared secret key, the method comprises:

receiving a key selection vector from a second digital platform in communication with the first digital platform; and

analyzing contents of the key selection vector from the second digital platform to determine the selected secret device keys of the first set of secret device keys.

(Previously Presented) 16. The method of claim 11, wherein prior to performing arithmetic operations on keys of at least two selected columns, the method further comprises:

dedicating the rows of the key matrix to a first classification; and

dedicating the columns of the key matrix to a second classification.

(Original) 17. The method of claim 11, wherein the producing of the shared secret key comprises:

analyzing contents of an incoming key selection vector; and

performing arithmetic operations of the selected secret device keys located in rows of the key matrix identified by the contents of the incoming key selection vector.

(Original) 18. The method of claim 17, wherein the producing of the shared secret key further comprises:

performing a hash operation on results of the arithmetic operations of the selected secret device keys located in the rows of the key matrix identified by the contents of the incoming key selection vector.

(Original) 19. A machine readable medium having embodied thereon a computer program for processing by a first digital platform including memory containing the computer program comprising:

an authentication function to recover an incoming key selection vector and to compute a shared secret key based on a set of secret device keys stored in the first digital platform and the contents of the incoming key selection vector;

a transfer function to output at least a key selection vector assigned to the first digital platform;

a hash function to perform a hash operation on at least the shared secret key to produce a resultant hash value; and

a comparison function to compare the resultant hash value with an incoming check hash value received subsequent to the transmission of the key selection vector.

(Original) 20. A network comprising:

a first digital platform; and

a certification authority in communication with the first digital platform, the certification authority having access to a key matrix featuring matrix keys arranged in accordance with at least a first dimension and a second dimension, generating a first key selection vector and providing a first set of secret device keys produced from selected matrix keys of the key matrix.

(Original) 21. The network of claim 20 further comprising:

a second digital platform in communication with the certification authority and the first digital platform, the second digital platform being uniquely assigned a second key selection vector indicating at least two grids of the key matrix and a second set of secret device keys produced from matrix keys situated in at least two grids of the key matrix.

(Original) 22. The network of claim 21, wherein the first and second digital platforms to exchange the first and second key selection vectors in order for each digital platform to produce a shared secret key to ensure that communications between the first and second digital platforms are secure.

(Original) 23. A certification authority comprising:

a memory to store a key matrix having N rows and M columns of matrix keys, where $N \geq 2$ and $M \geq 2$;

a logic to generate a key selection vector for each digital platform registered with the certification authority.

(Original) 24. The certification authority of claim 23, wherein the logic includes a processing unit.

(Original) 25. The certification authority of claim 24, wherein the processing unit produces a first set of secret device keys by performing arithmetic operations on matrix keys along selected

columns of the key matrix identificd by the key selection vector to provide a first set of secret device keys to a digital platform.

(Original) 26. The certification authority of claim 25, wherein the matrix keys along the processing unit performs arithmetic operations on matrix keys along selected rows of the key matrix identified by the key selection vector to provide a first set of secret device keys to a digital platform.

(Original) 27. The certification authority of claim 23, wherein the matrix keys are only known by the certification authority.

## APPENDIX B: EVIDENCE APPENDIX

To the best of Appellants' knowledge, there is no evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132 or of any other evidence entered by the examiner and relied upon by appellant in the present appeal that will directly affect, be directly affected by, or have a bearing on the Board's decision.

## APPENDIX C: RELATED PROCEEDINGS APPENDIX

To the best of Appellants' knowledge, there are no appeals or interferences related to the present appeal that will directly affect, be directly affected by, or have a bearing on the Board's decision.